

Offline Signature-Based Fuzzy Vault (OSFV): Review and New Results

George S. Eskander, Robert Sabourin and Eric Granger

École de technologie supérieure, Université du Québec

Montréal, Canada

Email: geskander@livia.etsmtl.ca, robert.sabourin@etsmtl.ca, eric.granger@etsmtl.ca.

This paper has been submitted to

The 2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM)

Abstract—An offline signature-based fuzzy vault (OSFV) is a bio-cryptographic implementation that uses handwritten signature images as biometrics instead of traditional passwords to secure private cryptographic keys. Having a reliable OSFV implementation is the first step towards automating financial and legal authentication processes, as it provides greater security of confidential documents by means of the embedded handwritten signatures. The authors have recently proposed the first OSFV implementation which is reviewed in this paper. In this system, a machine learning approach based on the dissimilarity representation concept is employed to select a reliable feature representation adapted for the fuzzy vault scheme. Some variants of this system are proposed for enhanced accuracy and security. In particular, a new method that adapts user key size is presented. Performance of proposed methods are compared using the Brazilian PUCPR and GPDS signature databases and results indicate that the key-size adaptation method achieves a good compromise between security and accuracy. While average system entropy is increased from 45-bits to about 51-bits, the AER (average error rate) is decreased by about 21%.

I. INTRODUCTION

Automation of financial and legal processes requires enforcement of confidentiality and integrity of transactions. For practical integration with the existing manual systems, such enforcement should be transparent to users. For instance, a person continually signs paper-based documents (e.g., bank checks) by hand, while his embedded handwritten signature images are used to secure the digitized version of the signed documents.

Such scenario can be realizable using biometric cryptosystems (also known as bio-cryptographic systems [1]) by means of the offline handwritten signature images. In bio-cryptography, biometric signals like fingerprints, iris, face or signature images, etc., secure private keys within cryptography schemes like digital signatures and encryption. Biometric samples provide a more trusted identification tool when compared to simple passwords. For instance, a fingerprint is attached to a person and it is harder to impersonate than traditional passwords.

Despite its identification power, biometrics forms a challenging design problem due to its fuzzy nature. For instance, while it is easy for a person to replicate his password during authentication, it rarely happens that a person applies exact

fingerprint each time. The main source of variability in physiological biometrics like fingerprint, face, iris, retina, etc. is the imperfect acquisition of the traits. On the other hand, behavioral biometrics like handwritten signatures, gait, and even voice, have intrinsic variability that is harder to cancel.

Fuzzy vault (FV) is a reliable scheme presented mainly to enable usage of fuzzy keys for cryptography [2]. A FV decoder permits limited variations in the decryption key so that secrets can be decrypted even with variable keys. Accordingly, this scheme fits the bio-cryptography implementations, where biometrics are considered as fuzzy keys by which private cryptographic keys are secured. Since the FV scheme has been proposed, it has been extensively employed for bio-cryptography, where most implementations focused on physiological biometrics, e.g., fingerprints [3], face [4] and iris [5]. FV implementations based on the behavioral handwritten signatures are few and mostly employed online signature traits, where dynamic features like pressure and speed are acquired in real time by means of special devices as electronic pens and tablets [6]. Static offline signature images, that are scanned after the signing process ends, however, integrate too much variability to cancel by a FV decoder [7].

Recently, the authors have proposed the first offline signature-based fuzzy vault (OSFV) implementation [8]-[12]. This implementation is employed to design a practical digital signature system by means of handwritten signatures [13]. In this paper, this implementation is reviewed and extended. In particular, we propose an extension to enhance the security and accuracy of the basic OSFV system by adapting cryptographic key size for individual users. Finally, system performance on the GPDS public signature database [14], besides the private PUCPR Brazilian database [15], are presented and interpreted.

The rest of the paper is organized as follows. In the next section, the OSFV implementation and its application to produce digital signatures by means of the handwritten signature images are reviewed. Section III describes the signature representation and lists some aspects for enhanced representations. Section IV introduces some OSFV variants for enhanced accuracy. Section V lists some variants for enhanced security. The new variant that adapts key sizes for enhanced security and accuracy is described in Section VI. The

simulation results are presented in Section VII. Finally, some research directions and conclusions are discussed in Section VIII.

II. FUZZY VAULTS WITH SIGNATURE IMAGES

The system proposed for OSFV consists of two main sub-systems: enrollment and authentication (see Figure 1). In the enrollment phase, some signature templates $\{T_s\}_{s=1}^S$ are collected from the enrolling user. These templates are used for the user representation selection, as described in Section III. The user representation selection process results in a user representations matrix $UR = (FI, VI, \Delta)$, where $FI = \{fI_i\}_{i=1}^t$ is the vector of indexes of the selected features, $VI = \{vI_i\}_{i=1}^t$ is a vector of indexes mapping represented in $l/2$ -bits¹, and $\Delta = \{\delta_i\}_{i=1}^t$ is the vector of expected variabilities associated with the selected features. This matrix is user specific and contains important information needed for the authentication phase. Accordingly, UR is encrypted by means of a user password PW . Both FV and password are then stored as a part of user bio-cryptography template (BCT). Then, the user parameters FI and VI are used to lock the user cryptography key K by means of a single signature template T_s in a fuzzy vault FV .

In the authentication phase, user password PW is used to decrypt the matrix UR . Then, the vectors FI, VI and Δ are used to decode the FV by means of user query signature sample Q . Finally, user cryptographic key K is released to the user so he can use it to decrypt some confidential information or digitally signs some documents.

A. Enrollment process

The enrollment sub-system uses the user templates $\{T_s\}_{s=1}^S$, the password PW , and the cryptography key K to generate a bio-cryptography template (BCT) that consists of the fuzzy vault FV and the encrypted user representation matrix EUR . The user representation selection module generates the UR matrix as described in Section III.

The OSFV encoding module (illustrated in Figure 2) describes the following processing steps:

- 1) the virtual indexes $VI = \{vI_i\}_{i=1}^t$ are quantized in $l/2$ -bits and produces a vector $X^T = \{x_i^T\}_{i=1}^t$.
- 2) the user feature indexes $FI = \{f_i\}_{i=1}^t$ are used to extract feature representation $F^T = \{f_i^T\}_{i=1}^t$ from the signature template T_s . This representation is then quantized in $l/2$ -bits and produces a vector $Y^T = \{y_i^T\}_{i=1}^t$.
- 3) The features are encoded to produce the locking set $A = \{a_i\}_{i=1}^t$, where $A = X^T || Y^T$ consists of l -bits FV points².
- 4) the cryptography key K of size KS where:

$$KS = l(k+1) - \text{bits} \quad (1)$$

¹As will be described later in this section, a feature index and its value are quantized in $l/2$ -bits each and then they are concatenated to produce a FV element of $l - \text{bits}$ size. Since a feature index fi might not fit in $l/2$ -bits, we map it in a virtual index v_i of a condensed size.

²FV points are represented with fixed quantization sizes since FV decoders rely on error-correction codes that employ finite (Galois) field computations.

is split into $k+1$ parts of l -bits each³, that constitutes a coefficient vector $C = \{c_0, c_1, c_2, \dots, c_k\}$. A polynomial p of degree k is encoded using C , where $p(x) = c_k x^k + c_{k-1} x^{k-1} + \dots + c_1 x + c_0$.

- 5) the polynomial is evaluated for all points in $A = \{a_i\}_{i=1}^t$ and constitutes the set $p(A) = \{p(a_i)\}_{i=1}^t$ where $p(a_i) = c_k a_i^k + c_{k-1} a_i^{k-1} + \dots + c_1 a_i + c_0$.
- 6) chaff (noise) points ($\hat{A} = \{\hat{a}_{ii}\}_{ii=t+1}^r, \hat{P} = \{\hat{p}_{ii}\}_{ii=t+1}^r$) are generated, where $\hat{a}_{ii} \in GF(2^l), \hat{a}_{ii} \neq a_i \vee ii \in [t+1, r], i \in [1, t]$, and $\hat{p}_{ii} \in GF(2^l), \hat{p}_{ii} \neq p(\hat{a}_{ii}) \vee ii \in [t+1, r]$. A chaff point $\hat{a}_{ii} = x_{ii} || y_{ii}$ is composed of two parts: the index part x_{ii} and the value part y_{ii} . Two groups of chaff points are generated. Chaffs of G_1 have their indexes equal to the indexes of the genuine points. The chaff points and the genuine point that have the same index part are all equally spaced by a distance Ω , eliminating the possibility to differentiate between the chaffs and the genuine point. Chaffs of G_2 have their index part differs than that of the genuine points⁴. As the number of chaffs in G_1 is limited by the parameters t and Ω , so to inject higher quantity of chaffs we define α as a chaff groups ratio, where:

$$\alpha = g_2/g_1 \quad (2)$$

where g_1 and g_2 are the amount of chaff features belong to G_1 and G_2 , respectively. G_2 chaffs are generated with αt indexes different than the t genuine indexes. Hence, the FV size r is given by:

$$r = t(\alpha + 1)/\Omega \quad (3)$$

So, the total number of chaffs z is given by:

$$z = t(\alpha + 1 - \Omega)/\Omega \quad (4)$$

- 7) the genuine set $(A, p(A))$, and the chaff set (\hat{A}, \hat{P}) are merged to constitute the fuzzy vault $FV = (A, \tilde{P})$, where $\tilde{A} = A \cup \hat{A}$, $A = \{a_i\}_{i=1}^t$, $\hat{A} = \{\hat{a}_i\}_{i=t+1}^r$ and $\tilde{P} = p(A) \cup \hat{P}$, $p(A) = \{p(a_i)\}_{i=1}^t$, $\hat{P} = \{\hat{p}_i\}_{i=t+1}^r$.

B. Authentication Process

The authentication sub-system uses the user query sample Q and the password PW , to decode the fuzzy vault FV and restore the user cryptography key K . First the password PW is used to decrypt the UR matrix. Then the vectors FI, VI , and Δ are used to decode the FV by means of the query Q .

The OSFV decoding module (illustrated in Figure 3) describes the following processing steps:

- 1) the virtual indexes $VI = \{vI_i\}_{i=1}^t$ are quantized in $l/2$ -bits and produces a vector $X^Q = \{x_i^Q\}_{i=1}^t$.

³The FV quantization size l is set to 16-bits in this work. So cryptographic keys of size $KS = 128$ -bits are encoded using polynomials of degree $k = 7$

⁴The user password protects the UR that stores his feature representation model. If the attacker compromised the password, the indexes of the genuine points are known to him. In such case, chaffs of G_2 are filtered out while G_1 could not be filtered without applying the good features.

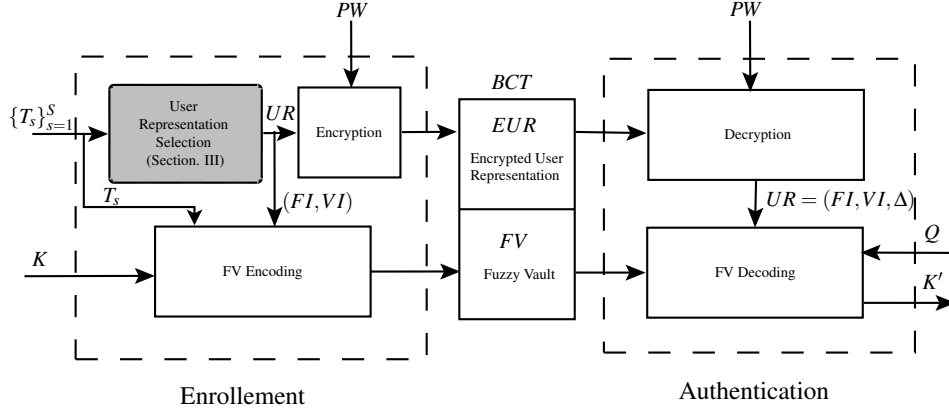


Fig. 1. Block diagram of the OSFV implementation [10].

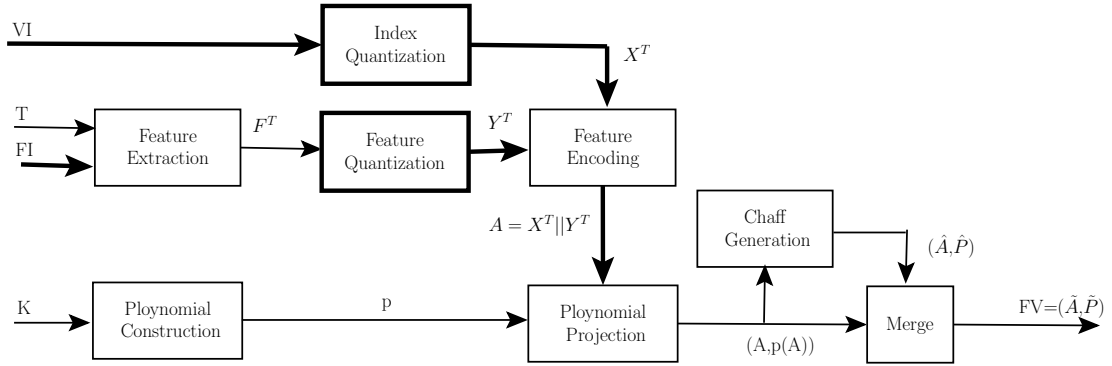


Fig. 2. Block diagram of the OSFV encoding process [10]. The bold lines highlight the modules where specific modifications apply to the standard encoding process employed in the literature of biometric FVs, e.g., [3].

- 2) the user feature indexes $FI = \{f_i\}_{i=1}^t$ are used to extract feature representation $F^Q = \{f_i^Q\}_{i=1}^t$ from Q . This representation is then quantized in $l/2$ -bits and produces a vector $Y^Q = \{y_i^Q\}_{i=1}^t$.
- 3) The features are encoded to produce the unlocking set $B = \{b_i\}_{i=1}^t$, where $B = X^Q || Y^Q$. Hence, the unlocking elements are represented in a field $GF(2^l)$.
- 4) the unlocking set B is used to filter the chaff points from the FV. An adaptive matching method is applied to match unlocking and locking points. Items of B are matched against all items in \tilde{A} . This process results in a matching set $(\tilde{A}, \tilde{P}) = ((B \cap \tilde{A}), p \leftarrow (B \cap \tilde{A}))$, where $p \leftarrow (B \cap \tilde{A})$ represents the projection of the matching features on the polynomial space. Chaff filtering is done as follows. If the feature indexes are correct⁵, then all elements of X^Q will have corresponding elements in X^T . So, all of chaffs of G_2 will be filtered out. Then, each of the remaining FV points will be compared to corresponding points extracted from the query sample. An adaptive matching method is applied: for every feature i , a matching window w_i is adapted to the feature

modeled variability δ_i , where $w_i = 2\delta_i$. A FV point a_i is considered matching with an unlocking point b_i , if they reside in the same matching window. I.e., $|a_i - b_i| \leq w_i$.

- 5) the matching set (\tilde{A}, \tilde{P}) is used to reconstruct a polynomial p' of degree k by applying the RS decoding algorithm [16].
- 6) the coefficients of p' are assembled to constitute the secret cryptography key K' .

C. Applications

In [13], the OSFV implementation is employed to produce digital signatures using offline handwritten signatures. This methodology facilitates the automation of business processes, where users continually employ their handwritten signatures for authentication. Users are isolated from the details related to the generation of digital signatures, yet benefit from enhanced security.

Figure 4 illustrates the OSFV-based digital signature framework. The user FV that is constructed during enrollment is used to sign user documents offline as follows. When a user signs a document by hand, his handwritten signature image is employed to unlock his private key d' . The unlocked key produces a digital signature by encrypting some message m extracted from the document (e.g., check amount). The

⁵That occurs if the applied password is genuine, so the UR is decrypted properly and the right indexes are restored.

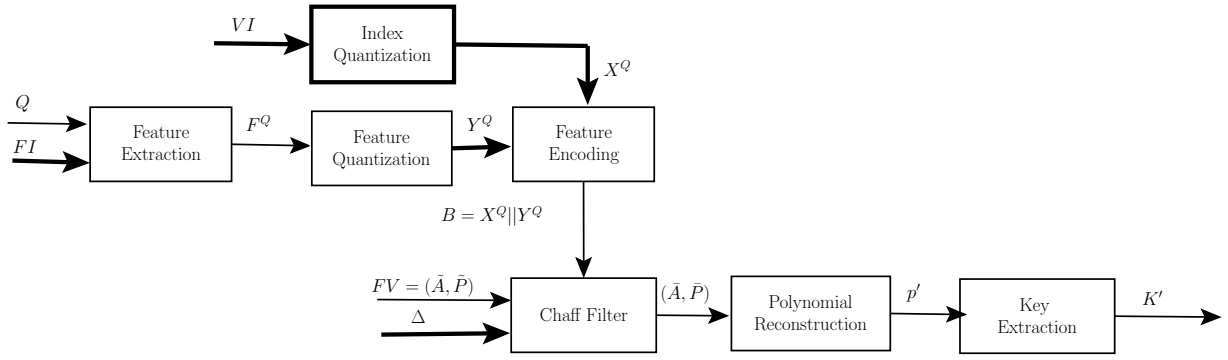


Fig. 3. Block diagram of the OSFV decoding process [10]. The bold lines highlight the modules where specific modifications apply to the standard encoding process employed in the literature of biometric FVs, e.g., [3].

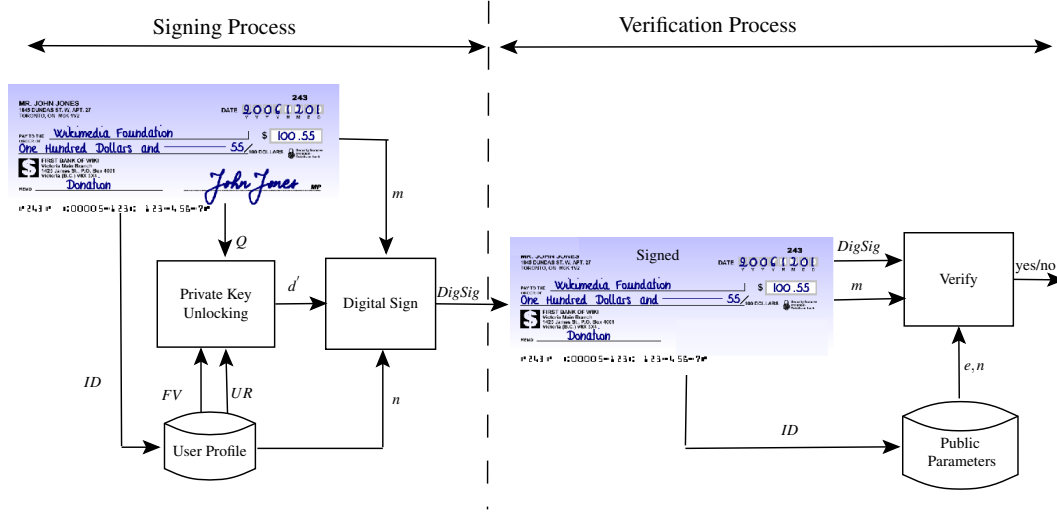


Fig. 4. Framework of a OSFV-based digital signature method [13].

encrypted message is considered as a digital signature and it is attached to the digitized document. Any party who possesses the user public key can verify the digital signature, where verification of the digital signature implies authenticity of the manuscript signature and integrity of the signed document (e.g., check amount did not change).

III. FEATURE REPRESENTATION

According to aforementioned OSFV implementation, the FV points encode some features extracted from the signature images. It is obvious that accuracy of a FV system relies on the feature representation. Representations of intra-personal signatures should sufficiently overlap so that matching errors lie within the error correction capacity of the FV decoder. On contrary, representations of inter-personal signatures should sufficiently differ so that matching errors are higher than the error correction capacity of the FV decoder.

Accordingly, the authors proposed to design signature representations adapted for the FV scheme by applying a feature selection process in a feature-dissimilarity space. In this space, features are extracted from each pair of template and query

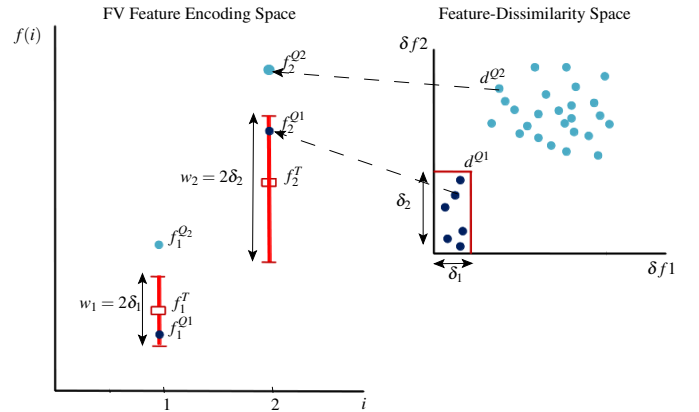


Fig. 5. Illustration of the feature representation designing process [10].

samples and the pair-wise feature distances are used as space dimensions.

To illustrate this approach, see Figure 5. In this example, three signature images are represented: T is the template signature, Q_1 is a genuine query sample and Q_2 is a forgery

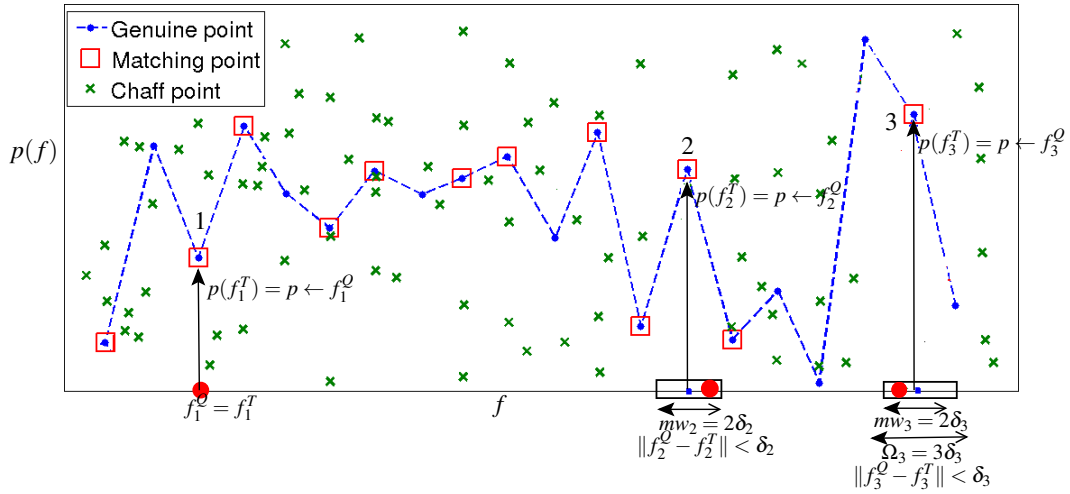


Fig. 6. Illustration of adaptive matching and adaptive chaff generation methods [11].

query sample. In the left side, signatures are represented in the FV feature encoding space, where a FV point encodes a feature index i and its value f_i . For simplicity, only two features (f_1 and f_2) are shown, while the full representation consists of t dimensions. On the right side, signatures are represented in the feature dissimilarity space. In this space, a feature is replaced by its distance from a reference value. For instance, f_1 and f_2 are replaced by their dissimilarity representations $\delta f_1, \delta f_2$, where $\delta f_1 = |f_1^Q - f_1^T|$, and $\delta f_2 = |f_2^Q - f_2^T|$. Accordingly, while a point in the feature encoding space represents a signature image, a point in the feature dissimilarity space represents the dissimilarity between two different signature images. The point d^{Q_1} represents the dissimilarity between the genuine signature Q_1 and the template T , and a point d^{Q_2} represents the dissimilarity between the forgery signature Q_2 and the template T , where $d^{Q_1} = (\delta f_1^{Q_1}, \delta f_2^{Q_1}, \dots, \delta f_t^{Q_1})$, and $d^{Q_2} = (\delta f_1^{Q_2}, \delta f_2^{Q_2}, \dots, \delta f_t^{Q_2})$.

In this example, δf_1 and δf_2 are discriminant features. For instance, for all genuine query samples like Q_1 , $\delta f_i^{Q_1} < \delta_i$ and for all forgery query samples like Q_2 , $\delta f_i^{Q_2} > \delta_i$. Unfolding these discriminant dissimilarity features to the original feature encoding space produces discriminant features in the encoding feature space, where the distance between two feature instances is used to determine their similarity. For instance, a genuine feature (like $f_i^{Q_1}$) lies close to the template feature f_i^T , so they are similar, where closeness here implies that both features reside in a matching window $w_i = 2\delta_i$. Features extracted from a forgery image (like $f_i^{Q_2}$) do not resemble the template feature f_i^T , as they reside outside the matching window w_i .

Aforementioned description of the process to design representations is generic. Some extensions are reviewed and compared below.

A. Global VS Local Representations

Shortage of user samples for training is addressed by designing a global writer-independent (WI) representation [8].

A large number of signature images from a development database are represented in the feature-dissimilarity space of high dimensionality, and feature selection process runs to produce a global space of reduced dimensionality. Such global approach permits designing FV systems for any user even who provides a single signature sample during enrollment.

For performance improvement, the global representation is specified for individual users once enough number of enrolling samples becomes available. To this end, training samples are firstly represented in the global representation space, then an additional training step runs to produce a local writer-dependent (WD) representation that discriminates the specific user from others. Simulation results have shown that local representations enhanced FV decoding accuracy by about 30%, where the average error rate (AER) is decreased from 25% in case of global representations to 17.75% for the local ones.

B. Multi-Scale Feature fusion

In [8], the Extended Shadow Code (ESC) feature extraction method is adapted for the FV implementation [18]. These features consist in the superposition of a bar mask array over a binary image of handwritten signatures. Each bar is assumed to be a light detector related to a spatially constrained area of the 2D signal. This method is powerful in detecting various levels of details in the signature images by varying the extraction scale. For instance, an image could be split to $h \times v$ of horizontal and vertical cells, respectively, and shadow codes are extracted within individual cells. The higher the number of cells, the higher the resolution of detectors.

The authors observed that designing FVs based on a single extraction scale results in varying performance for the different users. For instance, while high resolution scales are fine with users whose signatures are easy to forge or those who have high similarities with others, the low resolutions are better for users whose signatures integrate high variabilities. Accordingly, a multi-scale feature fusion method is proposed,

where different feature vectors are extracted based on different extraction scales and they are combined to produce a high-dimensional representation. This representation is then processed through the WI and WD design phased and produces the final local representation that encodes in the FV.

C. Multi-Type Feature fusion

Besides fusing feature vectors that are extracted based on different scales, it is possible to fuse different types of features. In [11], the directional probability density function (DPDF) features [19] are fused with ESC features to constitute a huge dimensional representation (of 30,201 dimensionality). This representation is reduced through the WI and WD training steps and produced a concise representation of only 20 features. It is shown that injecting the additional feature type increased the FV decoding accuracy by about 22% (AER is reduced from 17.75% to 13.75%).

D. Prototype Selection

The aforementioned approach provides a practical scenario to produce representations with low intra-personal and high inter-personal variabilities which is mandatory feature for FV systems. However, the authors observed that the margin between the intra and the inter classes differs when using different signature prototypes (templates) for FV encoding. Accordingly, a prototype selection method is proposed [9]. The WD representation is projected to a dissimilarity space where distances to different user prototypes are the space constituents. Then, a feature selection process runs in the dissimilarity space and locates the best prototype. This method has enlarged the separation between the intra and inter clusters significantly (Area under ROC curve (AUC) is increased from 0.93 to 0.97).

IV. EXTENSIONS FOR ENHANCED ACCURACY

Although accuracy of an OSFV system relies mainly on quality of the feature representation, the proposed implementation provides additional opportunities for enhanced accuracy by applying some other design variants as described in this section.

A. Adaptive Matching

The results mentioned so far report accuracy of FV decoders that apply strict matching approach. Two FV points are matching only if they have identical values. Accuracy of a FV decoder is enhanced by applying the adaptive matching method, where the feature variability matrix Δ is used for matching so that corresponding FV points are considered matching if their difference lies within the expected variability of their encoding feature (see Figure 6). This method increased accuracy by about 27% (AER is reduced from 13.75% to 10.08%) [10].

B. Ensemble of Fuzzy Vaults

Instead of decoding a single FV token, it is possible to decode several FVs for enhanced performance. In case that some FVs are correctly decoded, the decrypted key is released to the user based on the majority vote rule. This method has increased detection accuracy by about 18% (AER is reduced from 10.08% to 8.21%) [10].

C. Additional Passwords

The limited discriminative power of FVs is alleviated by using an additional password PW , so that the false accept rate (FAR) is reduced without significantly affecting the false reject rate (FRR). For the results reported so far, it was assumed that the user password PW is compromised. However, to report the actual performance of the system we have to consider the case when an attacker neither possesses a correct password nor a genuine signature sample. In this case, he cannot decrypt the UR model and hence he randomly guesses the feature indexes. It is shown that the additional password has increased detection accuracy by about 65% (AER is reduced from 8.21% to 2.88%) [10].

D. Cascading With Traditional SV Modules

Using additional passwords for enhanced system accuracy comes with the expense of the user inconvenience. In [12], a novel user-convenient approach is proposed for enhancing the accuracy of signature-based biometric cryptosystems. Since signature verification (SV) systems designed in the original feature space have demonstrated higher discriminative power to detect impostors [20], they can be used to improve the FV systems. Instead of using an additional password, the same signature sample is processed by a SV classifier before triggers the FV decoders (see Figure 7). Using this cascaded approach, the high FAR of FV decoders is alleviated by the higher capacity of SV classifiers to detect impostors. This method has increased detection accuracy by about 35% (AER is reduced from 10.08% to 6.55%). When multiple FVs are fused, the AER is decreased by 31.30% (from 8.21% to 5.64%).

V. EXTENSIONS FOR ENHANCED SECURITY

Security of the OSFV implementation is analyzed in terms of the brute-force attack [10]. Assume an attacker could compromise the FV without possessing neither valid password nor genuine signature sample. In this case, the attacker tries to separate enough number of genuine points ($k+1$) from the chaff points. Security of a FV is given by:

$$security \cong \binom{(\alpha+1)t}{k+1} (1/\Omega)^{k+1} \quad (5)$$

Where α is the chaff group ratio, t is the number of genuine points in the FV, k is the degree of the encoding polynomial and Ω is the chaff separation distance.

High value of α implies a high number of G2 features which are compromised in case that the password is compromised. The parameter t should be concise as it impacts the accuracy and complexity of the FV. Accordingly, entropy of the system

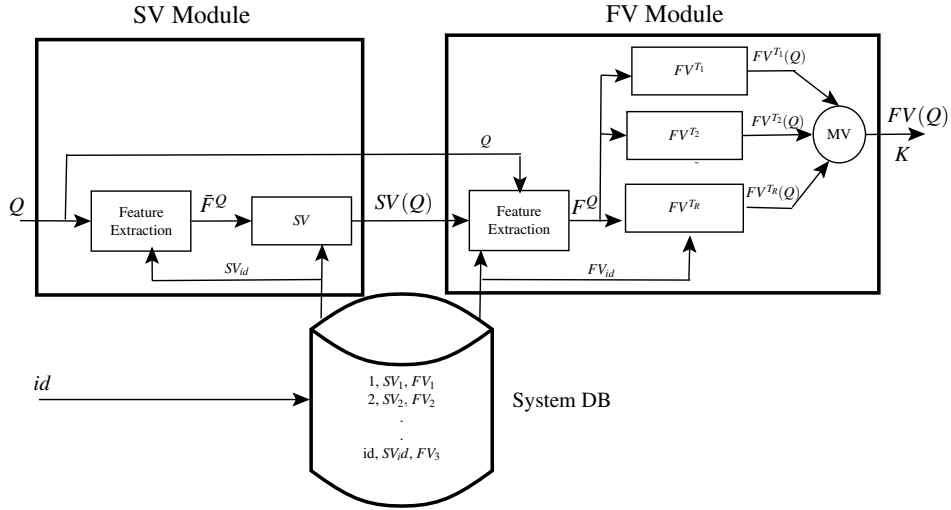


Fig. 7. Cascaded SV-FV system in the verification mode: different feature representations \bar{F} and F are processed by a SV classifier and a set of FV decoders, respectively. The FV module is triggered only if the SV module produces a positive classification label [12].

can be increased through using different values of the parameters: Ω and k . However, there is a trade-off between system security and its recognition accuracy that could be alleviated by applying the following approaches.

A. Adaptive Chaff Generation

In the traditional chaff generation method, equal-spaced chaff points are generated with a separation factor Ω [10]. In such case, there is a trade-off between security and robustness. For instance, with small separation, e.g., $\Omega = 0.025$, there are 40 FV points generated with the same index (1 genuine + 39 chaff points). In this case, a high number of chaffs is generated and results in high system entropy of about 68-bits and low accuracy of about 20% AER.

The adaptive chaff generation method enables the injection of high number of chaff with minimal impact on the FV decoding robustness. To this end, the feature variability vector Δ is used during the FV locking phase so that chaff points are generated adaptively according to feature variability. For each feature f_i , $\Omega_i = 3 \times \delta_i$ (see Figure 6). By this method, it is less likely that an unlocking element equates a chaff element. For or instance, the same entropy (68-bits) could be achieved with a minimal impact on system robustness (AER = 10.52%) [11].

B. Controlling Key Size

According to Eq.5, the longer the cryptographic key size the higher entropy of the FV. However, this comes with expense of the accuracy [10]. In [13], different key sizes (KS) are tried (128, 256, 512, 1024-bits) and it is shown that different key sizes result in different performance for the different users. This observation motivates adapting the key length for each user as proposed in the following section,

VI. THE ADAPTIVE KEY SIZE APPROACH

In [11], functionality of a FV decoder is formulated as a simple dissimilarity threshold as follows:

$$FV^T(Q) = \text{sign}(\epsilon - (\delta_A^{QT} + \delta')). \quad (6)$$

Where a FV encoded by a template T can be correctly decoded by a query Q only if the total dissimilarity between Q and T is less than the error correction capacity ϵ of the FV decoder. Here, δ_A^{QT} is the dissimilarity part that results from the variability between the two samples, and δ' is the dissimilarity part that results from wrong matches with chaff points.

The methods discussed so far aimed to optimize the dissimilarity parts of Eq.6. For instance, the multi-scale and multi-type feature extraction approach results in separating intra-personal and inter-personal dissimilarity ranges. Selection of robust templates (prototypes) and applying adaptive matching enlarged this separation. Also, impact of the chaff error is minimized by presenting the adaptive chaff method. With applying all these methods, however, accuracy of a signature-based FV is still below the level required for practical applications. Accordingly, performance is increased by applying some complex and user inconvenient solutions like ensemble of FVs and using additional passwords or cascading SV and FV systems.

Here we investigate a new room for enhancing FVs by optimizing the error correction capacity ϵ which is given by:

$$\epsilon = (t - k - 1)/2 \quad (7)$$

It is obvious that this parameter relies on the FV encoding size t and the encoding polynomial degree k . Also, from Eq.1, we see that k determines the key size KS . Accordingly, we select user specific key sizes through changing the parameter k so that ϵ for a specific user covers the range of his expected

signature variability. To this end, we set ε for a user to his maximum intra-personal variability e . Based on the resulting user-specific error correction capacity, the parameter k is determined using Eq.7 and user key size KS is computed using Eq.16.

Once appropriate key size is computed for a user, his key is enlarged through injecting some padding bits in the original key during FV encoding. During authentication, the enlarged key is reconstructed and the padding bits are removed to produce the original cryptographic key.

VII. SIMULATION RESULTS

All aforementioned performance results are reported for the PUCPR Brazilian signature database [15]. Here we test the system for the public GPDS-300 database [14] as well. This database contains signatures of 300 users, that were digitized as 8-bit greyscale at resolution of 300 dpi and contains images of different sizes (that vary from 51×82 pixels to 402×649 pixels). All users have 24 genuine signatures and 30 simulated forgeries. It is split into two parts. The first part contains signatures of the first 160 users. A subset of this part is used to design the local representation and the remaining of this part is used for performance evaluation. The second part contains signatures of the last 140 users and it is used to design the global representation. See [20] for a similar experimental protocol for both databases.

Table I shows results for the two databases for fixed and adaptive key sizes. It is obvious that employing the adaptive key size approach decreased the FAR significantly with low impact on the FRR. For instance, the AER for the PUCPR database is decreased by about 21% (from 10.08 to 7.94). Also, performance of the system for the GPDS database is comparable to state-of-the-art traditional SV systems (AER is about 15%) that employ more complex classifiers [20].

Moreover, the proposed method also enhances system security as it is possible to increase the key size, and hence the polynomial degree k , without much impact on the accuracy. For instance, Figure 8 shows the adapted polynomial degrees for different users in the PUCPR database and the corresponding user variability e . It is obvious that users with more stable signatures have their cryptographic keys more enlarged than users with less stable signatures. According to Eq.5, system entropy of the standard OSFV implementation (with fixed keys of size 128-bits and polynomial degree $k = 7$) is about 45-bits. With applying the adaptive key size method, the average k is about 9.6-bits (see Figure 8) which provides an average entropy of about 51-bits.

VIII. CONCLUSIONS AND RESEARCH DIRECTIONS

In this paper, a recently published offline signature-based FV implementation is reviewed. Several variants of the system are listed and compared for enhanced accuracy and security. A novel method to adapt cryptography key sizes for different users is proposed and have shown accuracy and security

⁶In this work, we set an upper limit for the error correction capacity to be $\varepsilon \leq 6$ so that $k \geq 7$ and $KS \geq 128$ -bits.

TABLE I
IMPACT OF USING A USER PASSWORD AS A SECOND AUTHENTICATION MEASURE

Measure	PUCPR DB		GPDS DB	
	Fixed Key	Adaptive Key	Fixed Key	Adaptive Key
FRR	11.53	12.71	37.5	39.07
FAR_{random}	2.05	0	0	0
FAR_{simple}	2.39	0.05	-	-
$FAR_{simulated}$	24.28	19.02	15.37	11.20
AER_{all}	10.08	7.94	17.6	16.75

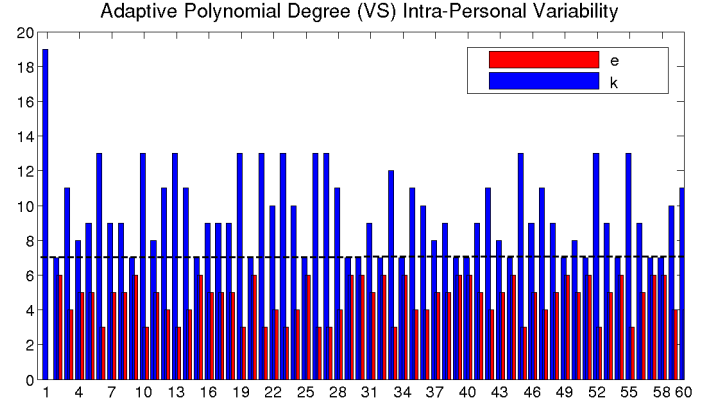


Fig. 8. Adaptive polynomial degree (k) VS Intra-personal variability (e)

enhancement. The performance is also validated on a public signature database where comparable results of complex SV in the literature is reported. Although the proposed key adaptation method sounds, there is need to propose more intelligent tuning technique taking in consideration the similarities with simulated forgeries for higher forgery detection. This study listed many new approaches that are applied successfully to the signature based bio-cryptography. We believe that these methods shall be investigated for other biometrics which might enhance state-of-the-art of the area of bio-cryptosystems.

REFERENCES

- [1] U. Uludag, S. Kantian, S. Mahabharata and A.K. Jain., Biometric Cryptosystems: Issues and Challenges. *Prof. of the IEEE*, vol.92, no.6, pp.948-960, 2004.
- [2] A. Jules and M. Sudan., A Fuzzy Vault scheme. *In crop. IEEE int. Sump. Inf. Theory*, Switzerland, pp.408, 2002.
- [3] K. Nandakumar A. K. Jain and S. Kantian., Fingerprint Based Fuzzy Vault: Implementation and Performance. *IEEE Trans. on Information Forensic and Security*, vol.2, no.4, pp.744-757, 2007.
- [4] Y. Wang and KN. Plataniotis., Fuzzy Vault for Face based cryptographic key generation. *Biometrics Symposium*, Baltimore, Maryland, USA, pp.1-6, 2007.
- [5] Y. J. Lee and K. R. Park, S. J. Lee, K. Bae, and J. Kim., A new method for generating an invariant iris private key based on the Fuzzy Vault system. *IEEE Transactions on Systems, Man, and Cybernetics- part B: Cybernetics*, vol.38, no.5, pp.1302-1313,
- [6] M. Freire-Santos, J. Fierrez-Aguilar and J. Ortega-Garcia., Cryptographic key generation using handwritten signatures. *proc of SPIE*, vol.6202, pp.225-231, 2006.
- [7] Manuel Freire-Santos, J. Fierrez-Aguilar, M. Martinez-Diaz and J. Ortega-Garcia., On the applicability of off-line signatures to the Fuzzy Vault construction. *proc of ICDAR2007*, Curitiba, Brazil, 2007.

- [8] G.S. Eskander., R. Sabourin, and E. Granger, Signature based Fuzzy Vaults with boosted feature selection. *IEEE Workshop on Computational Intelligence and Identity Management (SSCI-CIBIM 2011)*, pp.131-138, Paris, 2011.
- [9] G.S. Eskander., R. Sabourin, and E. Granger, On the Dissimilarity Representation and Prototype Selection for Signature-Based Bio-Cryptographic Systems. *2nd Int'l. Workshop on Similarity-Based Pattern Analysis and Recognition*, York, UK, 3-5 July 2013, LNCS, vol.7953, pp.265-280.
- [10] G.S. Eskander., R. Sabourin, and E. Granger, Bio-Cryptographic System Based on Offline Signature Images. *Information Sciences*, vol 259, 2014, pp 170-191, 2014.
- [11] G.S. Eskander., R. Sabourin, and E. Granger, A Dissimilarity-Based Approach for Biometric Fuzzy Vaults—Application to Handwritten Signature Images. *Int'l Workshop on Emerging Aspects in Handwritten Signature Processing*, Naples, Italy, September 2013.
- [12] G.S. Eskander., R. Sabourin, and E. Granger, Improving Signature-Based Biometric Cryptosystems Using Cascaded Signature Verification-Fuzzy Vault (SV-FV) Approach. *14th International Conference on Frontiers in Handwriting Recognition (ICFHR-2014)*, Crete Island, Greece, 1-4 September 2014.
- [13] G.S. Eskander., R. Sabourin, and E. Granger, Towards Automated Transactions based on the Offline Handwritten Signatures. *9th International Conference on Machine Learning and Data Mining (MLDM'2013)*, New York, USA, July 2013.
- [14] J. Vargas, M. Ferrer, C. Travieso, J. Alonso., Off-line handwritten signature GPDs-960 corpus. *International Conference on Document Analysis and Recognition*, pp.764-768, 2007.
- [15] C. Freitas, M. Morita, L. Oliveira, E. Justino, A. Yacoubi, E. Lethelier, F. Bortolozzi and R. Sabourin., Bases de dados de cheques bancarios brasileiros. *XXVI Conferencia Latinoamericana de Informatica*, Mexico, 2000.
- [16] Berlekamp and Elwyn R., Algebraic Coding Theory. *McGraw-Hill*, New York, NY, USA, 1968.
- [17] Rivard, D, Granger, E and Sabourin, R., Multi-Feature extraction and selection in writer-independent offline signature verification. *International Journal on Document Analysis and Recognition*, vol.16, no.1, pp.83-103, 2013.
- [18] R. Sabourin and G. Genest., An Extended-Shadow-Code based Approach for Off-Line Signature Verification. *Proc of the 12th international conference on Pattern Recognition*, Jerusalem, vol.2, pp.450-453, 1994.
- [19] J. Drouhard, R. Sabourin and M. Godbout., A neural network approach to off-line signature verification using directional pdf. *Pattern Recognition*, vol.29, no.3, pp.415-424, 1996.
- [20] G. Eskander, R. Sabourin, and E. Granger. 2013. "Hybrid Writer-Independent-Writer-Dependent Offline Signature Verification System". *IET-Biometrics Journal, Special issue on Handwriting Biometrics*, vol.2, no.4, pp. 169 -181